基于改进的 Cat 置乱与 Henon_Kent 混沌系统的彩色图像自适应加密算法 *

谢国波，陈志伟

(广东工业大学 计算机学院，广州 510006)

摘　要：为了解决彩色图像加密算法中密钥与明文图像不关联的安全性不足以及 Cat 映射成立条件的问题，提出一种基于改进的 Cat 置乱系统与 Henon_Kent 混沌扩散系统的彩色图像自适应加密算法。该算法首先利用明文图像特征信息生成密钥；然后通过改进的 Cat 置乱系统对图像进行像素位置的三维置乱，再将 Henon_Kent 混沌系统所产生的三个混沌序列分别对 RGB 三个通道的像素灰度值进行扩散；重复以上两个步骤，以密文图像的信息熵大于 7.99 为结束条件。仿真表明该算法能够抵抗现有的攻击方法，具有较强的加密性能。

关键词：图像加密；Cat 置乱；Henon_Kent 混沌系统；自适应加密

中图分类号：TP309.7　　doi: 10.3969/j.issn.1001-3695.2018.04.0314

Color image adaptive encryption algorithm based on improved Cat scrambling and Henon_Kent chaotic system

Xie Guobo, Chen Zhiwei

(*School of Computers Guangdong University of Technology, Guangzhou* 510006, *China*)

Abstract: In order to solve the problem of the lack of security associated with the key and the plaintext image in the color image encryption algorithm, and conditions for the establishment of Cat maps, proposed a color image adaptive encryption algorithm based on improved Cat scrambling system and Henon_Kent chaotic diffusion system. The algorithm firstly used the feature information of plaintext image to generation key; secondly, used the improved Cat scrambling system to perform the three-dimensional scrambling of pixel positions; then three chaotic sequences generated by the Henon_Kent chaotic system were used to spread the pixel gray values of the three channels of RGB respectively; repeated the above two steps to ensure that the entropy of the ciphertext image is greater than 7.99. The simulation shows that this algorithm can resist the existing attack methods and has strong encryption performance.

Key words: image encryption; cat scrambling; Henon_Kent chaotic system; adaptive encryption

0　引言

近几年，在人们工作和生活中互联网得到广泛地应用，其中包含数字音频、数字图像和其他多媒体信息传输，数字图像的安全传递问题变得越来越重要。使用传统的 AES(高级加密标准算法)、DES（数据加密标准加密算法）、RSA（公钥加密算法）算法对数据图像加密需要大量的计算时间，而且存在潜在的缺点。

混沌系统具有伪随机性和对初始值敏感性的特点，基于混沌系统的图像加密算法被许多学者相继提出[1~4]。由于使用单一低维混沌的算法密钥空间较小和安全性较差，不能抵抗常见的攻击。文献[5]提出一种基于混合混沌系统的彩色图像加密算法，使用两个混沌系统有利于增加密钥空间，但由于彩色图像只进行一维和二维的位置置乱，安全性有待进一步提高。文献[6]提出一种基于 3D Cat 映射的图像加密算法，将二维图像扩展到三维进行 3D Cat 映射，但加密密钥没有与明文图像相关联，因此不能有效地抵抗选择密文（明文）攻击。文献[7]提出了一种新的基于混合混沌映射和动态随机生长技术的块图像加密方案，解决了 Cat 映射的周期性问题，有效地抵制了选择的明文攻击；但对于一个行列式和 *n* 不互质的等长图像或一个 *m/n* 为非整数比的非等长图像，如果进行二维 Cat 映射，图像将不能进行一一对应映射，且造成映射位置重复的像素缺失。文献[8~10]通过增加行列形成一个 M*M 的图像来解决 Cat 映射所构成的条件，该操作将会增加密文图片的存储大小，同时密文图

收稿日期：2018-04-26；**修回日期：**2018-06-20　　**基金项目：**广东省科技计划资助项目（2016B030306004，2015B020233019）；广州市科技计划资助项目（201604016041）

作者简介：谢国波（1977-），男，广东五华人，教授，博士，主要研究为混沌保密通信、分布式处理系统（guoboxie@163.com）；陈志伟（1993-），男，广东佛山人，硕士研究生，主要研究方向为混沌加密、图像处理.

像在网络通信时所需的资源成比例增加。

针对以上部分加密算法存在的密钥与明文图像不关联以及 Cat 置乱条件的问题，本文提出一种基于改进的 Cat 置乱系统与 Henon_Kent 混沌扩散系统的彩色图像自适应加密算法。其中改进的 Cat 置乱系统将三维 Cat 映射的一对一映射的规则改为灰度值的互换，解决了 Cat 映射的条件问题。本文加密算法首先利用彩色明文图像的特征信息产生复合混沌系统的密钥；然后将彩色明文图像像素通过改进的 Cat 置乱系统进行三维空间置乱，像素三维空间交换使彩色图像的灰度值均匀分布在 R、G 和 B 三个分量中。本文提出的 Henon_Kent 混沌系统产生三个混沌加密序列与三维置乱后的彩色图像 R、G 和 B 三个通道的像素灰度值进行扩散。重复以上两个步骤，直到密文图像的安全性分析达到一定的标准才结束。本文算法采取三维空间置乱—像素扩散的自适应循环结构。实验仿真表明，本文算法具有比较好的抗统计分析攻击能力和抗差分攻击等能力。

1　本文加密算法原理

本文提出了一种基于改进的 Cat 置乱系统与 Henon_Kent 混沌扩散系统的彩色图像自适应加密算法，其流程如图 1 所示。其中可大致分为四个主要部分：a)与彩色明文图像相关的密钥生成；b)改进的 Cat 系统的置乱方法；c)Henon_Kent 混沌扩散方法；d)自适应循环系统。

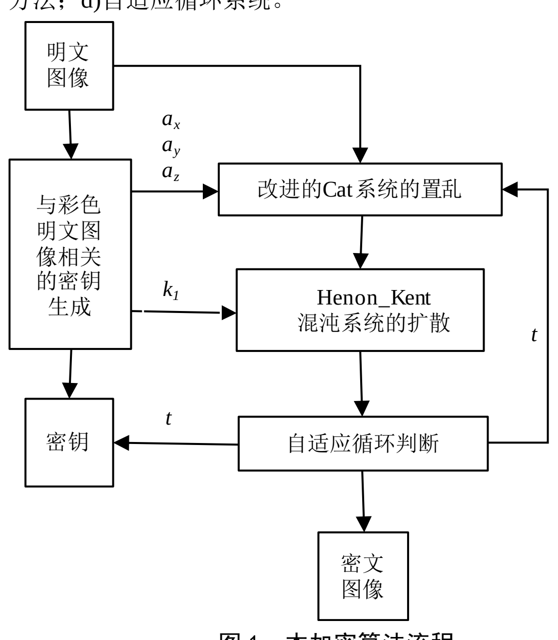


图 1　本加密算法流程

彩色图像的尺寸大小为 m×n×3 的三维矩阵。为了方便算法的描述，设矩阵 A 表示为 m×n×3 的彩色明文图像，$A(i,j,k)$ 表示彩色明文图像坐标为 (i,j,k) 的值。

1.1　与彩色明文图像相关的密钥生成

本文算法的加密密钥不是直接生成，而是与明文特征相关。由式（1）可得 *A* 的带位置参数像素灰度值和为 *sum*，式（2）可得 Kent 映射的初始值 k_1，式（3）~（5）可得改进的三维 Cat 置乱系统的初始值 a_x、a_y、a_z。

$$sum=\sum_{i}^{m}\sum_{j}^{n}\sum_{k}^{3}(A(i,j,k)+i+j+k) \tag{1}$$

$$k_1=\frac{\mathrm{mod}(sum,m*n*3)}{m*n*3} \tag{2}$$

$$a_x=\mathrm{round}(\mathrm{mod}(k_1*10^5,10))+1 \tag{3}$$

$$a_y=\mathrm{round}(\mathrm{mod}(k_1*10^6,10))+1 \tag{4}$$

$$a_z=\mathrm{round}(\mathrm{mod}(k_1*10^7,10))+1 \tag{5}$$

1.2　改进的 Cat 系统的置乱

二维广义 Cat 映射又称为 Arnold 映射，其表达式如式（6）所示。

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}1 & b\\a & ab+1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\mathrm{mod}(N) \tag{6}$$

其中：(x,y) 表示灰度图像的原像素点位置，经过二维 Cat 映射到 (x',y') 的位置；$\mathrm{mod}(N)$ 表示限制在 $[0,N]$ 之间。关于二维的广义 Cat 映射的条件：等长图像置乱变换阵对应的行列式和 *n* 互质；非等长图像的 *m/n* 为整数比，则 Cat 变换存在周期性[11]。

针对 Cat 映射成立的条件问题，本文提出改进的三维 Cat 置乱系统。该系统采用三维 Cat 映射[12]，将一对一映射的规则改为灰度值的互换，解决了 Cat 映射的周期性和映射条件问题，其定义如式（7）所示。

$$\begin{cases}x' = \mathrm{mod}(A_{11}x+A_{12}y+A_{13}z,m)+1\\ y' = \mathrm{mod}(A_{21}x+A_{22}y+A_{23}z,n)+1\\ z' = \mathrm{mod}(A_{31}x+A_{32}y+A_{33}z,3)+1\end{cases} \tag{7}$$

其中：
$$\begin{cases}A_{11}=1+a_xa_ya_z\\ A_{12}=a_z\\ A_{13}=a_y+a_xa_z+a_xa_ya_zb_y\\ A_{21}=b_z+a_xa_y+a_xa_zb_yb_z\\ A_{22}=a_zb_z+1\\ A_{23}=a_ya_z+a_xa_za_yb_yb_z+a_xa_zb_z+a_xa_yb_y+a_x\\ A_{31}=a_xb_xb_z+1\\ A_{32}=b_x\\ A_{33}=a_xa_yb_xb_y+a_xb_x+a_yb_y+1\end{cases}$$

对于彩色图像的尺寸大小为 m×n×3，像素位置为 (x,y,z) 经过式（7）的计算得出的位置 (x',y',z')，$x'\in[1,m]$，$y'\in[1,n]$，$z'\in[1,3]$，使 (x,y,z) 的像素灰度值与 (x',y',z') 的像素灰度值交换，而非进行矩阵的映射。改进的三维 Cat 交换具有非周期性，彩色图像经过多次改进的三维 Cat 交换，图像像素点在 R、G 和 B 三个分量中均匀分布，像素点之间具有很强的不相关性，从而达到更好的加密效果和抗攻击能力。

该方法的具体步骤如下：

a）通过式（2）~（4）选定式（7）的参数 a_x、a_z、a_y，另

外自行选定式（7）的部分密钥 b_x、b_z、b_y 。

b）(*u*，*v*，*w*)为从矩阵 *A* 的(1，1，1)位置开始到(m，n，3)结束。遵循矩阵行优先、列次之和 RGB 后的原则，矩阵 *A* 的位置(*u*，*v*，*w*)经过式（7）计算得出位置(*u'*，*v'*，*w'*)，然后将 *A*(*u*，*v*，*w*)与 *A*(*u'*，*v'*，*w'*)两者灰度值交换。

c）将置乱后的图像 *A* 转换成 R、G、B 三个分量对应的二维灰度矩阵 *Ar*、*Ag*、*Ab*，其中每个矩阵的大小为 m×n。

1.3 Henon_Kent 混沌系统的扩散

本文算法提出的 Henon_Kent 混沌系统是将 Henon 映射产生的两个混沌序列和 Kent 映射产生的一个混沌序列进行运算生成三个混合混沌序列。

Henon 映射相比普通的映射具有更强的对初始条件敏感性和更好的动力学系统的特性，其定义为式(8)所示。

$$\begin{cases} x_{s+1} = y_s + a * x_s^2 + 1 \\ y_{s+1} = b * x_s \end{cases} \quad s \in \{1, 2, \ldots\} \qquad (8)$$

其中：a、b 为 Henon 映射的控制参数。混沌系统至少有一个正的 Lyapunov 指数，对于一个系统处于稳定定态和周期运动时，不可能具有正的 Lyapunov 指数，Henon 系统具有两个正的 Lyapunov 指数，当 $1.54 < a < 2$，$0 < |b| < 1$ 时，系统经过多次迭代进入混沌状态[12]。

Kent 映射是一维混沌系统，其定义如式(9)所示。

$$k_{s+1} = \begin{cases} k_s / d & k_s \in (0, d] \\ (1 - k_s)/(1 - d) & k_s \in (0, d] \end{cases} \quad s \in \{1, 2 \ldots\} \qquad (9)$$

其中：d 为该混沌系统的控制参数。当 $k_1 \in (0,1), d \in (0,1)$ 时，Kent 映射具有一个正的 Lyapunov 指数，系统处于混沌状态。

Henon_Kent 映射是使用以上两个映射（Henon 映射和 Kent 映射）所产生的混沌序列进行运算产生三个混沌序列，其定义如式(10)所示。

$$\begin{cases} r_s = (x_s + k_s) * \partial \bmod 256 \\ g_s = (y_s + k_s) * \beta \bmod 256 \\ b_s = (x_s + y_s + k_s) * \gamma \bmod 256 \end{cases} \quad s \in \{1, 2, 3..\} \qquad (10)$$

其中：∂，β，γ 为控制参数；mod 为取余操作；r_s、g_s 和 b_s 为产生的混沌序列，其值域范围在[0,1]区间内。Henon_Kent 映射对彩色图像的加密可大大增强 R、G、B 三个分量对密钥的敏感性，其产生的混沌序列比非联合多混沌系统产生的混沌序列对初始状态更敏感，从而提升加密算法整体的安全性。对 Henon_Kent 混沌系统进行仿真，迭代 1 000 次的分布图如图 2 所示。

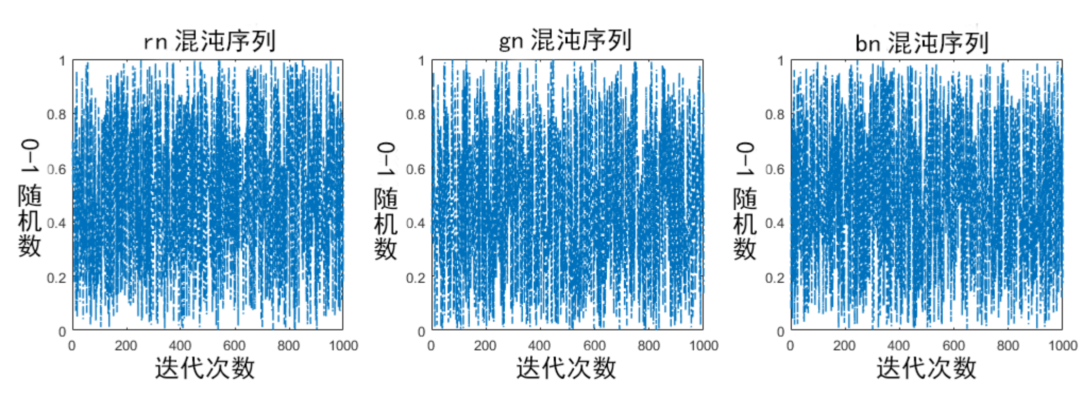


图 2　Henon_Kent 混沌系统迭代分布图

该方法的具体步骤如下：

a）为 Henon 映射的式（8）和 Kent 映射的式（9）选定合适的参数和初始值，其中利用式（5）计算得出式（9）的 Kent 映射初始值 k_1，迭代次数为 s 以消除暂态效果，然后迭代 m×n 次可得到长度为 m×n 三组混沌序列 x_s、y_s、k_s，其中 $s = (1, 2, 3, \ldots, m * n)$，应用设定特定参数的式（10）对 x_s、y_s、k_s 三个序列进行操作得到三个序列 r_s、g_s、b_s 。

b）对 r_s、g_s、b_s 三个序列进行操作形成三个尺寸为 m×n 的二维矩阵，分别与 *Ar*、*Ag*、*Ab* 三个矩阵的像素灰度值进行异或操作，形成三个中间密文分量 *Mr*、*Mg*、*Mb*。

1.4 自适应循环判断

为了实现明文彩色图像经过置乱与扩散后，达到一定的加密效果，同时防止算法过多的循环次数，本文采取以密文图像的信息熵为加密效果的评判标准。

信息熵可以衡量图像灰度值的分布情况，图像的信息熵越大，表明图像的图像灰度值分布越均匀。其公式如式（11）所示。

$$H(m) = -\sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \qquad (11)$$

其中：$P(m_i)$ 为图像中灰度 i 出现的概率，当密文图像的信息熵接近 8 时，说明密文图像具有伪随机性和高安全性，加密算法能够抵抗熵攻击。

该方法的具体步骤如下：

a）获得中间密文分量 Mr、Mg、Mb，分别通过式（11）计算三个中间密文的信息熵 $H(Mr)$、$H(Mg)$、$H(Mb)$。

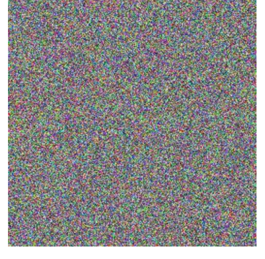
b）当 $H(Mr)$、$H(Mg)$、$H(Mb)$ 都大于 7.99 时，结束循环算法，并以循环的次数 t 作为密钥；否则重复改进的 Cat 系统的置乱和 Henon_Kent 混沌系统的扩散方法，同时 $t = t+1$。

1.5　算法的密文解密过程

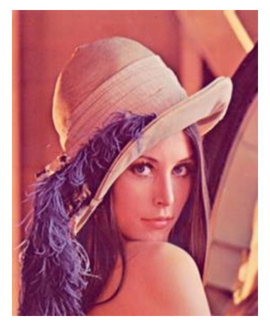
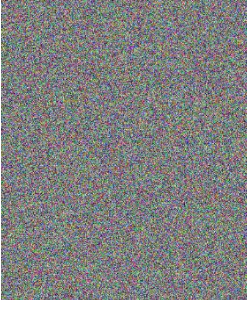
图像解密过程是上述图像加密步骤的逆过程。

2　实验仿真及安全性分析

本文算法仿真采用大小为 256*256*3 的彩色 Lena 图像（图 3(a)）以及大小为 500*400*3 的彩色 Lena 图像（图 3(c)）作为明文图像。为了与其他算法进行更好对比，本文安全性分析以图 3(a)为主、图 3(d)为辅。本文算法密钥为：Henon_Kent 混沌系统的扩散中 Henon 映射初始值为 $x_0 = 0.501334562$、$y_0 = 0.554157444$，控制参数为 $a = 1.2$、$b = 0.3$，Kent 映射的初始值 $k_0 = 0.6006$ 与明文特征关联及其控制参数 $d = 0.4$，式（10）的控制参数为 $\partial = 10^5$、$\beta = 10^5$、$\gamma = 10^5$。改进的三维 Cat 系统的置乱中控制参数 $a_x = 1$、$a_y = 2$、$a_z = 3$ 与明文特征关联以及其他控制参数 $b_x = 4$、$b_y = 5$、$b_z = 6$。算法最终的循环次数 t=2。经过仿真明文图像图 3(a)经过本文算法仿真结果的密文图像如图 3(b)所示，图 3(c)的密文图像如图 3(d)所示。

(a) 明文图像　　(b) 图像(a)的密文图像

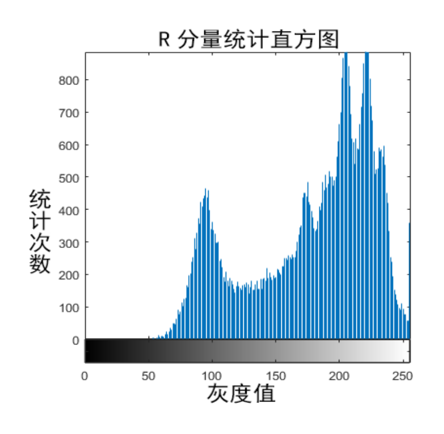



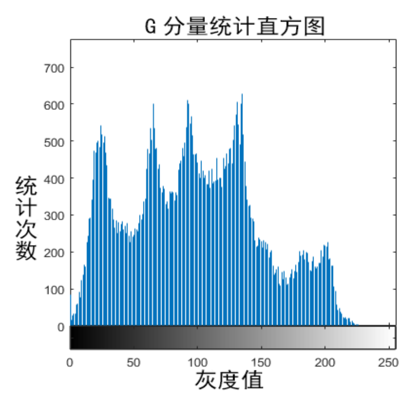
(c) 明文图像　　(d) 图像(c)的密文图像

图 3　图像加密结果

2.1　图像统计直方图

明文图像图 3(a)的统计直方图如图 4 所示，密文图像图 3(b)的统计直方图如图 5 所示，图 3(c)的统计直方图如图 6 所示，密文图像图 3(d)的统计直方图如图 7 所示。结果表明 R、G、B 分量的统计直方图分布均匀，各个灰度值统计总量相近，从而实现加密明文图像的目的。





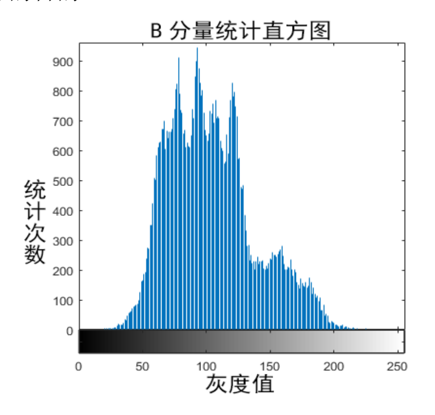
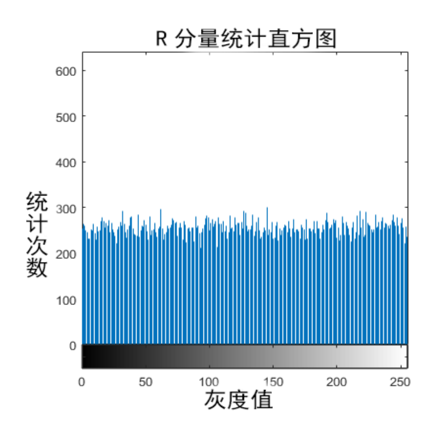
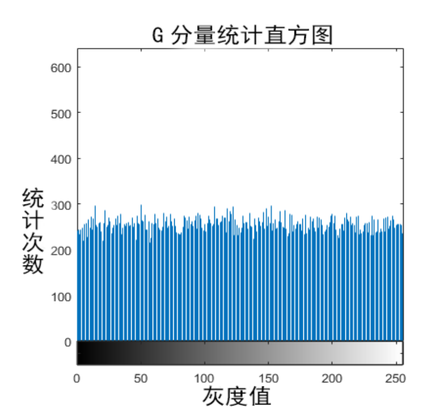


图 4　明文图像图 3(a)统计直方图





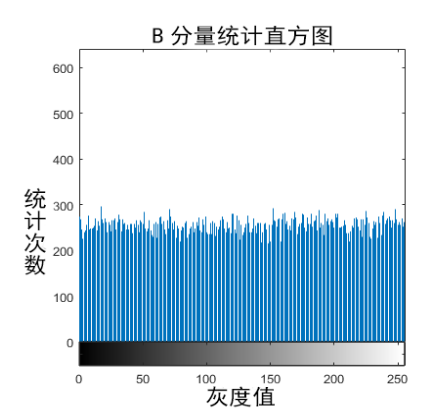
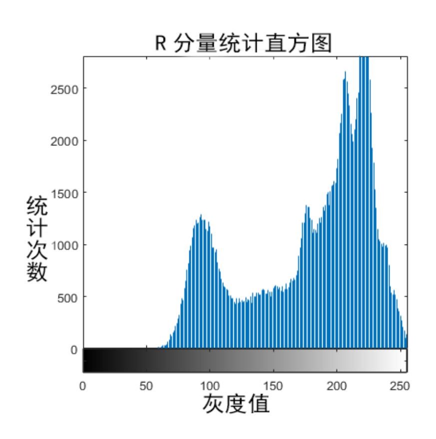
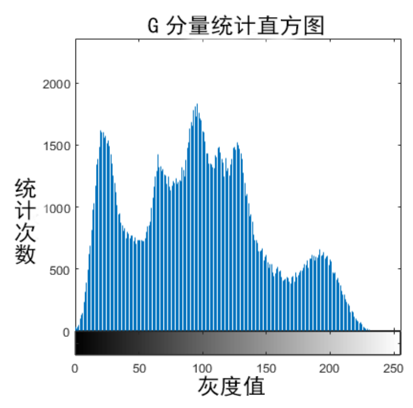


图 5　密文图像图 3(b)的统计直方图





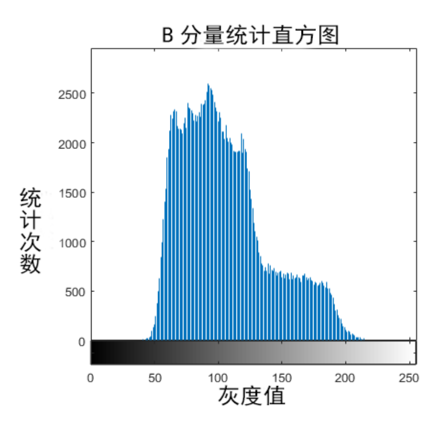
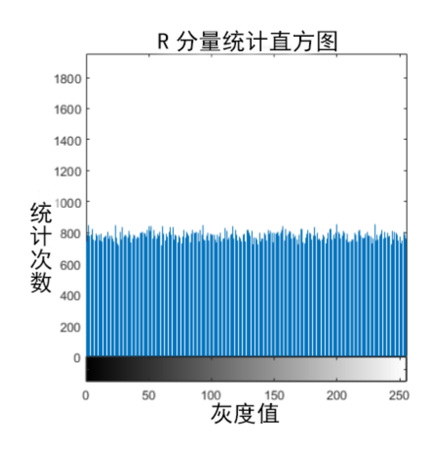
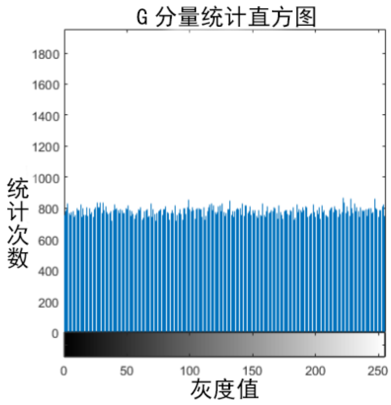


图 6　明文图像图 3(c)的统计直方图





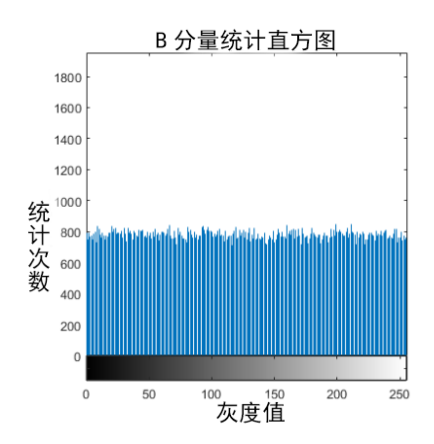


图 7　密文图像图 3(d)的统计直方图

2.2　图像相邻像素相关性分析

图像相邻像素相关性分析是分别从水平、垂直和对角线三个方向计算图像相邻像素相关系数，加密后的密文图像的像素相关性越低且接近为零，反映出图像加密效果好，加密算法抵抗相邻像素相关性统计攻击能力强。相邻像素相关系数计算公式为如式（12）～（14）和式（15）所示。

$$\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{12}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2 \tag{13}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y}) \tag{14}$$

$$\gamma_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{15}$$

其中：γ_{xy} 为相邻像素相关性系数。通过本文算法得出密文图像和文献[13]、文献[14]的相关性系数如表 1 所示。本文加密算法加密后的密文图像相关性系数接近 0，与文献[13]和文献[14]相比，相当一部分值更小。因此，本文加密算法具有更强的抗相关性分析攻击能力。

表 1　相邻像素相关性系数

		R 分量	G 分量	B 分量
图 3(a)	水平	0.9719	0.9745	0.9455
	垂直	0.9337	0.9414	0.8943
	对角	0.8989	0.9161	0.8519
图 3(a)的密文图像	水平	-0.0142	-0.0253	0.0062
	垂直	0.0077	-0.0051	0.0026
	对角	0.0168	0.0179	-0.0006
文献[13]密文图像	水平	0.0206	-0.0005	0.0016
	垂直	-0.0116	-0.0002	0.0189
	对角	0.0097	0.0133	-0.0123
文献[14]	水平	-0.0104	-0.0029	0.0123

密文图像	垂直	0.0095	0.0126	0.0116
	对角	0.0215	0.0135	0.0304
	水平	0.0075	−0.0149	−0.0031
图 3(d)	垂直	−0.0037	−0.0104	0.0186
	对角	−0.0185	0.0266	−0.0003

2.3　密钥空间分析

本文加密算法采用多轮多混沌系统对彩色图像进行加密。改进的三维 Cat 置乱算法输入的密钥采用长整型，Henon_Kent 混沌系统输入的密钥采用双精度运算。改进的三维 Cat 置乱算法中控制参数 a_x、a_z、a_y、b_x、b_z、b_y 密钥空间为 10^9。像素扩散算法中 Henon 映射初始值为 x_0 和 y_0，密钥空间为 10^{20}，控制参数为 a、b，密钥空间为 10^3，Kent 映射的初始值为 k_0，密钥空间为 10^{10}。式(7)的控制参数 ∂、β 和 γ 密钥空间为 10^{30}。本文加密算法输入的密钥空间接近 $10^{70} > 2^{200}$，有效地抵抗了穷举的攻击破解本文加密算法，从而增加了算法的安全性。

2.4　明文敏感性分析

明文敏感性分析是指图像中像素灰度值发生微小变化时，加密后的图像产生截然不同的变化。产生的变化一般采用 NPCR (像素变化率)和 UACI (归一化像素平均值)来检测。NPCR 和 UACI 计算方法如式（16）和（17）所示。

$$NPCR = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{i=1}^{N} D(i,j) \times 100\% \tag{16}$$

$$UACI = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{i=1}^{N}\frac{|A_1(i,j) - A_2(i,j)|}{255} \times 100\% \tag{17}$$

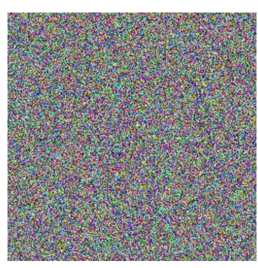
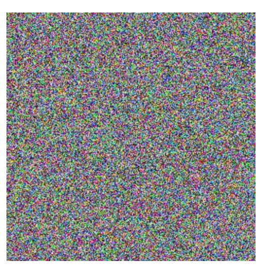
其中：$D(i,j)$ 代表如果图像 A_1 和 A_2 在 (i,j) 位置的灰度值相同时则 $D(i,j)=1$，否则 $D(i,j)=0$；$A_1(i,j)$ 代表图像 A_1 在 (i,j) 位置的灰度值。本文算法的密钥与明文的像素灰度值相关联。对于 256*256*3 的彩色 Lena 图像 A_1，将 A_1 随机选择一个像素进行加 1 操作为新彩色 Lena 图像 A_2，将 A_1 和 A_2 进行 NPCR 和 UACI 计算。经过多次仿真计算得出 R、G 和 B 分量的 NPCR 和 UACI 平均值以及文献 15 的值，如表 2 所示。表 2 可以得出本文算法 NPCR>99.6%和 UACI>33.3%，本文的加密算法对于明文的特性具有高度敏感。

表 2　NPCR 和 UACI 平均值及对比

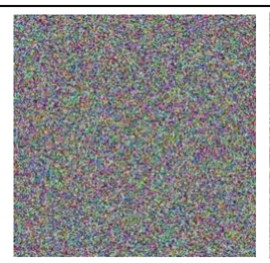
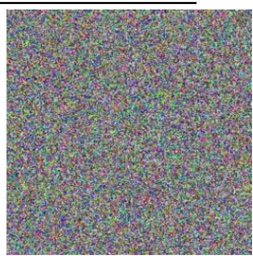
		R 分量	G 分量	B 分量
本文算法	NPCR	99.63%	99.65%	99.60%
文献[15]	NPCR	99.65%	99.62%	99.58%
本文算法	UACI	33.42%	33.48%	33.35%
文献[15]	UACI	33.48%	33.41%	33.34%

2.5　密钥敏感性分析

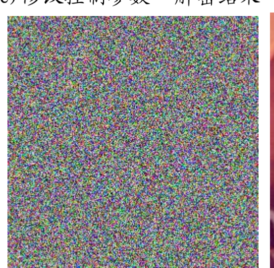
密钥敏感性是指对密钥进行微小的改变时，解密得出图像不存在明文特征信息的图像。本文对所有的密钥进行严谨的仿真，分别对所有的密钥进行独立且微小的修改，可得图 3(b)解密结果如图 8 所示，其中图 8(a) (b)分别为 Henon_Kent 混沌系统中式（8）Henon 映射初始值 $x_0 = 0.501934561$ 修改为 $x_0 = 0.501934562$、控制参数 $a = 1.25$ 修改为 $a = 1.26$ 的解密结果；(c) (d)分别为像素扩散算法中式（9）控制参数 $d = 0.4$ 修改为 $d = 0.5$、式（10）的控制参数 $\partial = 10^{10}$ 修改为 $\partial = 10^{10} + 1$ 的解密结果；(e)为改进的 Cat 置乱系统的置乱算法中控制参数 $a_x = 1$ 修改为 $a_x = 2$ 的解密结果；(f)为不修改密钥的解密结果。

(a) 修改密钥 x_0 解密结果　(b) 控制参数 a 解密结果

(c) 修改控制参数 d 解密结果　(d) 修改控制参数 ∂ 解密结果



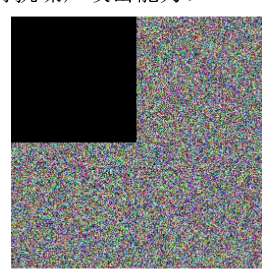
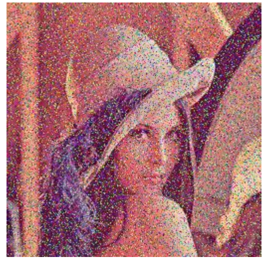

(e) 修改控制参数 a_x 解密结果　(f) 正确密钥解密结果

图 8　密钥敏感性分析

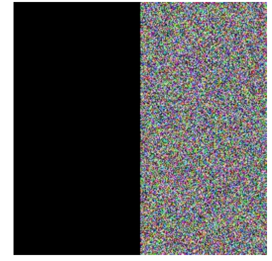
2.6　抗剪切能力分析

实现抗剪切能力分析需要通过模拟图像传输过程中图像局部信息丢失来，本文对密文图像图 3(b)进行 25%和 50%的截切如图 9 (a)和 (c)所示，图 9(a)和(c)的解密图像分别为图 9(b)和(d)所示，如图 9 (c)为将 R 分量的灰度值全设为 255，图(c)的解密

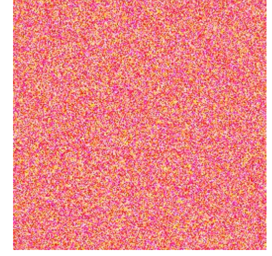
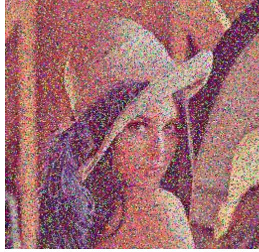
图像为图(f)所示。以上仿真结果显示本文加/密解密算法在图像传输过程信息丢失情况下能把图像解密，且解密结果能够显示明文图像的部分信息，通过剪切能力分析同时可以得到本文算法具有抗噪声攻击能力。

(a)25%剪切密文图像 (b)25%剪切密文图像解密结果




(c)50%剪切密文图像 (d)50%剪切密文图像解密结果

(e)R 分量剪切密文图像(f)R 分量剪切密文图像解密结果

图 9 抗剪切攻击能力分析

3 结束语

本文提出一种基于改进的Cat置乱系统与Henon_Kent混沌扩散系统的彩色图像自适应加密算法。与其他加密算法对比，本文算法具有以下特点：a)针对彩色图像本文提出一种改进的Cat 置乱算法，解决了传统的 Cat 映射的成立条件和周期性问题，可以在不改变图像的尺寸下进行图像的像素置乱，随着迭代次数的增加，使图像的像素更随机地分布在密文图像的 R、G 和 B 分量中；b)本文使用一种新的 Henon_Kent 混沌系统，该混沌系统产生混沌序列具有更强的动力学特性和伪随机性，有效地对明文图像进行像素的扩散，使像素均匀地分布在[0, 255]之间。通过仿真，本文算法具有强鲁棒性，针对各种攻击手段具有比较强的抵抗能力。

参考文献：

[1] El-Assad S, Farajallah M. A new chaos-based image encryption system [J]. Signal Processing Image Communication, 2016, 41: 144-157.

[2] Liu Hongjun, Wang Xingyuan. Color image encryption based on one-time keys and robust chaotic maps [J]. Computers & Mathematics with Applications, 2010, 59 (10): 3320-3327.

[3] Wang Xingyuan, Yang Lei, Liu Rong, *et al.* A chaotic image encryption algorithm based on perceptron model [J]. Nonlinear Dynamics, 2010, 62 (3): 615-621.

[4] Liu Hongjun, Wang Xingyuan, Kadir A. Image encryption using DNA complementary rule and chaotic maps [J]. Applied Soft Computing, 2012, 12 (5): 1457–1466.

[5] Wang Leyuan, Song Hongjun, Liu Ping. A novel hybrid color image encryption algorithm using two complex chaotic systems [J]. Optics & Lasers in Engineering, 2016, 77: 118-125.

[6] Chen Guanrong, Mao Yaobin, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos Solitons & Fractals, 2004, 21 (3): 749-761.

[7] Wang Xingyuan, Liu Lintao, Zhang Yingqian. A novel chaotic block image encryption algorithm based on dynamic random growth technique [J]. Optics & Lasers in Engineering, 2015, 66: 10-18.

[8] Ding Ma, Jing Fan. Digital image encryption algorithm based on improved Arnold transform [C]// Proc of International Forum on Information Technology and Applications. Piscataway, NJ: IEEE Press, 2010: 174-176.

[9] 李国辉，张松岭，吴成茂. 一种改进时空混沌的图像加密算法 [J]. 西安邮电大学学报，2017，22 (3): 44-49. (Li Guohui, Zhang Songling, Wu Chengmao. An image encryption algorithm based on improving spatiotemporal chaos [J]. Journal of Xian University of Posts & Telecommunications, 2017, 22 (3): 44-49.)

[10] 田汉清，全吉成，程红，等. 一种结合 Cat 映射和 Henon 映射的图像加密技术 [J]. 计算机应用与软件，2010，27 (9): 286-288. (Tian Hanqing, Quan Jicheng, Cheng Hong, *et al.* An image encryption scheme combining cat map and henon map. Computer Applications & Software. [J]. Computer Applications & Software, 2010, 27 (9): 286-288.)

[11] 邵利平，覃征，高洪江，等. 二维非等长图像置乱变换 [J]. 电子学报，2007, 35 (7): 1290-1294. (Zhao Liping, Tan Zheng, Gao Hongjiang, *et al.* 2-D Arnold transformation and non-equilateral image scrambling transformation [J]. Acta Electronica Sinica Computer, 2007, 35 (7): 1290-1294.)

[12] Mohamed N A, El-Azeim M A, Zaghloul A, *et al.* Image encryption scheme for secure digital images based on 3D cat map and Turing machine [C]// Proc of the 7th International Conference of Soft Computing and Pattern Recognition. Piscataway, NJ: IEEE Press, 2015: 230-234.

[13] Wu Xiangjun, Wang Dawei, Kurths J, *et al.* A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system [J]. Information Sciences, 2016, 349: 137-153.

[14] Tong Xiaojun, Zhang Miao, Wang Zhu, *et al.* A joint color image encryption and compression scheme based on hyper-chaotic system [J]. Nonlinear Dynamics, 2016, 84 (4): 2333-2356.

[15] Niyat A Y, Moattar M H, Torshiz M N. Color image encryption based on hybrid hyper-chaotic system and cellular automata [J]. Optics & Lasers in Engineering, 2017, 90: 225-237.